

**AMENDMENT #1 TO  
MEMORANDUM OF AGREEMENT BETWEEN  
THE KANSAS DEPARTMENT OF CORRECTIONS (KDOC)  
& KIM DAUGHERTY**

This Amendment #1 is made to the Memorandum of Agreement between the Kansas Department of Corrections (KDOC) and Kim Daugherty (Contractor) effective December 1, 2012. (Contract).

The parties agree to the following:

1. KDOC has provided Contractor access to the KDOC information systems including Offender Management Information System (OMIS) and Total Offender Activity Documentation (TOADS) for reading and/or entering information about offenders as needed to deliver services under the aforesaid Contract. Contractor agrees that she will abide by all rules, regulations, policies and procedures related to use of the information and confidentiality, and will execute necessary paperwork so agreeing before being provided access. Specifically, Contractor shall undergo the training in NCIC and KCJIS policies and procedures required in the KCJIS Security Addendum which is attached hereto, incorporated herein, and marked as Amendment Attachment A; and shall execute the individual agreement form – “Federal Bureau of Investigation Criminal Justice Information Services Security Addendum” – therein. And be provided a copy of, read, and sign agreeing to abide by the provisions of the Security Awareness Statement at Amendment Attachment A. Copies of these signed items shall be maintained in

Contractor's personal file, and copies shall be forwarded to the KDOC designated point of contact in the aforesaid Contract.

2. Contractor shall at all times comply with the National Standards promulgated under the Prison Rape Elimination Act (42 U.S.C. §15601, et seq.), which are found at 28 CFR 115.5 to 115.93, inclusive, and the provisions of KDOC Internal Management Policy and Procedure (IMPP) 10-103, in regard to any of its employees who have or may reasonably be expected to have contact with inmates in delivering services and/or goods pursuant to this agreement.

a. In particular, Contractor shall:

1. Prior to going into a KDOC correctional facility to perform her duties, submit name and necessary identifying information to the KDOC for a criminal background check, and repeat this process at 5-year intervals as required by 28 CFR 115.17; and also shall be subject to any necessary inquiry with past employers as to any involvement in any incident of sexual misconduct set forth at subsection (a) thereof, also per 28 CFR 115.17 at subsection (a);
2. promptly make herself available for orientation and periodic training provided by KDOC in regard to the obligations and requirements imposed by said Act and National Standards, as required by 28 CFR 115.32 and IMPP 10-103, Sec. II;

3. participate in any KDOC sexual abuse incident review conducted pursuant to 28 CFR 115.86 in which Contractor is involved as the target of the investigation and review, or a witness thereto, for interview by the Sexual Abuse Incident Review Board, as well as any pertinent records regarding the incident in question; and
  4. promptly make available upon request any records necessary for KDOC to meet the requirements for data collection, review for corrective action, and audits, as set forth at 28 CFR 115.87, 115.88, 115.93.
- b. Contractor further acknowledges that KDOC must bar any contract employee found to have engaged in sexual abuse from its facilities' premises, as well as report any such employee to law enforcement agencies and relevant licensing bodies, and that KDOC otherwise must take appropriate remedial measures in response to any violation of its sexual abuse or sexual harassment policies, as set forth at 28 CFR 115.77. Contractor further acknowledges and agrees that KDOC, in its sole discretion, may bar any contract employee under investigation for alleged sexual abuse or sexual harassment during the investigation.
3. The provisions found in the updated Contractual Provisions Attachment (Form DA-146a), which is attached hereto as Amendment Attachment B are incorporated in this Amendment #1 and made part hereof. Should any of the provisions of this Amendment #1 or the aforesaid Contract conflict with any

provisions of the Contractual Provisions Attachment, the provisions set forth  
in the Contractual Provision Attachment shall control.

IN WITNESS WHEREOF, the parties hereto have caused this Amendment #1 to  
be executed by their duly authorized representatives the day and year indicated  
below.

STATE OF KANSAS

KIM DAUGHERTY

By: \_\_\_\_\_  
Ray Roberts, Secretary

By: \_\_\_\_\_  
Kim Daugherty

Date: \_\_\_\_\_

Date: \_\_\_\_\_

**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the  
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
  - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
  - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
  - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

**1.00 Definitions**

**1.01 Contracting Government Agency (CGA)** - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

**1.02 Contractor** - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

**2.00 Responsibilities of the Contracting Government Agency.**

**2.01** The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgment may be signed by hand or via digital signature (see glossary for definition of digital signature).

**3.00 Responsibilities of the Contractor.**

**3.01** The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

**4.00 Security Violations.**



4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

#### 5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

#### 6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

\_\_\_\_\_  
Printed Name/Signature of Contractor Employee

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name/Signature of Contractor Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Organization and Title of Contractor Representative

## Security Awareness Statement

Only authorized personnel are allowed to have unrestricted access to some areas of the facilities or to have access into any data processing systems that may process, store, or transmit KCJIS-sensitive information.

- Be familiar with restricted access areas, how authorized personnel are identified, and proper procedure to safely challenge unknown unrecorded persons.

Not all security threats involve technology. Some examples and prevention steps are listed below.

- Social Engineering occurs when individuals present themselves as someone they are not (such as a repairman, delivery person, or other service personnel). They will then engage you in conversation in hopes of collecting confidential information regarding individuals, events or details of technologies in use, etc.

To prevent Social Engineering, never discuss agency specific information with anyone other than authorized agency personnel.

- To prevent unauthorized access, misuse or pre-mature destruction of media (printed documents, hard drives, magnetic tapes, etc.) all media must be stored in a secure manner when not in use. Also be aware of environmental hazards such as storing media near heat sources or liquids.
- To prevent unauthorized access to confidential information once the agency has no further use of it. The media containing that information must be disposed of or sanitized according to KCJIS Policies and Procedures.

If you notice media that appears to be out of place you should alert your agency supervisor or other responsible agency personnel immediately.

Report any situation you suspect may be a security risk to your agency supervisor or other responsible agency personnel immediately.

Misuse of KCJIS information may result in disciplinary action, including immediate dismissal, or may even subject you to civil and criminal penalties including a fine up to \$11,000.

Your signature below certifies that you:

- Have read this document,
- I have read any parts relevant to your association with this agency of the following:  
1) The agency's Standard Operating Procedures manual,  
2) The KCJIS Policy and Procedure Manual,
- Agree to abide with the provisions of this document and other relevant documents,
- Understand the consequences of violating agency or KCJIS policies.

\_\_\_\_\_  
Associate Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature for the Agency

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Agency Designation

☐ Check box when appropriate if background screening checks are complete.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Initials

## Security Awareness Statement

Only authorized personnel are allowed to have unrestricted access to some areas of the facilities or to have access into any data processing systems that may process, store, or transmit KCJIS-sensitive information.

- Be familiar with restricted access areas, how authorized personnel are identified, and proper procedure to safely challenge unknown or suspected persons.

Not all security threats involve technology. Some examples and prevention steps are listed below.

- Social Engineering occurs when individuals present themselves as someone they are not (such as a repairman, delivery person, or other service personnel). They will then engage you in conversation in hopes of collecting confidential information regarding individuals, events or details of technologies in use, etc.

To prevent Social Engineering, never discuss agency specific information with anyone other than authorized agency personnel.

- To prevent unauthorized access, misuse or pre-mature destruction of media (printed documents, hard drives, magnetic tapes, etc.) all media must be stored in a secure manner when not in use. Also be aware of environmental hazards such as storing media near heat sources or liquids.
- To prevent unauthorized access to confidential information once the agency has no further use of it. The media containing that information must be disposed of or sanitized according to KCJIS Policies and Procedures.

If you notice media that appears to be out of place you should alert your agency supervisor or other responsible agency personnel immediately.

Report any situation you suspect may be a security risk to your agency supervisor or other responsible agency personnel immediately.

Misuse of KCJIS information may result in disciplinary action, including immediate dismissal, or may even subject you to civil and criminal penalties including a fine up to \$11,000.

Your signature below certifies that you:

- Have read this document,
- Have read any parts relevant to your association with this agency of the following:
  - 1) The agency's Standards Operating Procedures manual,
  - 2) The KCJIS Policy and Procedure Manual,
- Agree to abide with the provisions of this document and other relevant documents,
- Understand the consequences of violating agency or KCJIS policies.

\_\_\_\_\_  
Associate Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature for the Agency

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Agency Official Name



Check box when appropriate personnel screening checks are complete.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Initials

## AMENDMENT ATTACHMENT B

State of Kansas

Department of Administration

DA-146a (Rev. 4-11-13 KDOC)

### CONTRACTUAL PROVISIONS ATTACHMENT

**Important:** This form contains mandatory contract provisions and must be attached to or incorporated in all copies of any contractual agreement. If it is attached to the vendor/contractor's standard contract form, then that form must be altered to contain the following provision:

"The Provisions found in Contractual Provisions Attachment (Form DA-146a, Rev. 04-11), which is attached hereto, are hereby incorporated in this contract and made a part thereof."

The parties agree that the following provisions are hereby incorporated into the contract to which it is attached and made a part thereof, said contract being the \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_\_.

1. **Terms Herein Controlling Provisions:** It is expressly agreed that the terms of each and every provision in this attachment shall prevail and control over the terms of any other conflicting provision in any other document relating to and a part of the contract in which this attachment is incorporated. Any terms that conflict or could be interpreted to conflict with this attachment are nullified.
2. **Kansas Law and Venue:** This contract shall be subject to, governed by, and construed according to the laws of the State of Kansas, and jurisdiction and venue of any suit in connection with this contract shall reside only in courts located in the State of Kansas.
3. **Termination Due to Lack of Funding Appropriation or Budget Rescission or Allotment:** If, in the judgment of the Director of Accounts and Reports, Department of Administration, sufficient funds are not appropriated to continue the function performed in this agreement and for the payment of the charges hereunder, State may terminate this agreement at the end of its current fiscal year. State agrees to give written notice of termination to contractor at least 30 days prior to the end of its current fiscal year, and shall give such notice for a greater period prior to the end of such fiscal year as may be provided in this contract, except that such notice shall not be required prior to 90 days before the end of such fiscal year. If, in the judgment of the Secretary of the state agency party, as a result of a budget rescission ordered by the Governor, or a budget allotment ordered by the Secretary of Administration, insufficient funds remain to support the function performed in this agreement and for payment of charges hereunder, State may terminate this agreement upon giving 30 days' written notice. In the event of termination due to any circumstance set forth above, Contractor shall have the right to take possession of any equipment provided State under the contract, upon the effective date of termination. State will pay to the contractor all regular contractual payments incurred up to the effective date of termination, plus contractual charges, if any, incidental to the return of any such equipment. Upon termination of the agreement by the State, title to any such equipment shall revert to the contractor upon the effective date of termination. The termination of the contract pursuant to this paragraph shall not cause any penalty to be charged to the agency or the contractor.
4. **Disclaimer Of Liability:** No provision of this contract will be given effect that attempts to require the State of Kansas or its agencies to defend, hold harmless, or indemnify any contractor or third party for any acts or omissions. The liability of the State of Kansas is defined under the Kansas Tort Claims Act (K.S.A. 75-6101 et seq.).
5. **Anti-Discrimination Clause:** The contractor agrees: (a) to comply with the Kansas Act Against Discrimination (K.S.A. 44-1001 et seq.) and the Kansas Age Discrimination in Employment Act (K.S.A. 44-1111 et seq.) and the applicable provisions of the Americans With Disabilities Act (42 U.S.C. 12101 et seq.) (ADA) and to not discriminate against any person because of race, religion, color, sex, disability, national origin or ancestry, or age in the admission or access to, or treatment or employment in, its programs or activities; (b) to include in all solicitations or advertisements for employees, the phrase "equal opportunity employer"; (c) to comply with the reporting requirements set out at K.S.A. 44-1031 and K.S.A. 44-1116; (d) to include those provisions in every subcontract or purchase order so that they are binding upon such subcontractor or vendor; (e) that a failure to comply with the reporting requirements of (c) above or if the contractor is found guilty of any violation of such acts by the Kansas Human Rights Commission, such violation shall constitute a breach of contract and the contract may be cancelled, terminated or suspended, in whole or in part, by the contracting state agency or the Kansas Department of Administration; (f) if it is determined that the contractor has violated applicable provisions of ADA, such violation shall constitute a breach of contract and the contract may be cancelled, terminated or suspended, in whole or in part, by the contracting state agency or the Kansas Department of Administration.

Contractor agrees to comply with all applicable state and federal anti-discrimination laws.

The provisions of this paragraph number 5 (with the exception of those provisions relating to the ADA) are not applicable to a contractor who employs fewer than four employees during the term of such contract or whose contracts with the contracting State agency cumulatively total \$5,000 or less during the fiscal year of such agency.

6. **Acceptance Of Contract:** This contract shall not be considered accepted, approved or otherwise effective until the statutorily required approvals and certifications have been given.
7. **Arbitration, Damages, Warranties:** Notwithstanding any language to the contrary, no interpretation of this contract shall find that the State or its agencies have agreed to binding arbitration, or the payment of damages or penalties. Further, the State of Kansas and its agencies do not agree to pay attorney fees, costs, or late payment charges beyond those available under the Kansas Prompt Payment Act (K.S.A. 75-6403), and no provision will be given effect that attempts to exclude, modify, disclaim or otherwise attempt to limit any damages available to the State of Kansas or its agencies at law, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

8. **Representative's Authority To Contract:** By signing this contract, the representative of the contractor thereby represents that such person is duly authorized by the contractor to execute this contract on behalf of the contractor and that the contractor agrees to be bound by the provisions thereof.
9. **Responsibility For Taxes:** The State of Kansas and its agencies shall not be responsible for, nor indemnify a contractor for, any federal, state or local taxes which may be imposed or levied upon the subject matter of this contract.
10. **Insurance:** The State of Kansas and its agencies shall not be required to purchase any insurance against loss or damage to property or any other subject matter relating to this contract, nor shall this contract require them to establish a "self-insurance" fund to protect against any such loss or damage. Subject to the provisions of the Kansas Tort Claims Act (K.S.A. 75-6101 et seq.), the contractor shall bear the risk of any loss or damage to any property in which the contractor holds title.
11. **Information:** No provision of this contract shall be construed as limiting the Legislative Division of Post Audit from having access to information pursuant to K.S.A. 46-1101 et seq.
12. **The Eleventh Amendment:** "The Eleventh Amendment is an inherent and incumbent protection with the State of Kansas and need not be reserved, but prudence requires the State to reiterate that nothing related to this contract shall be deemed a waiver of the Eleventh Amendment."
13. **Campaign Contributions / Lobbying:** Funds provided through a grant award or contract shall not be given or received in exchange for the making of a campaign contribution. No part of the funds provided through this contract shall be used to influence or attempt to influence an officer or employee of any State of Kansas agency or a member of the Legislature regarding any pending legislation or the awarding, extension, continuation, renewal, amendment or modification of any government contract, grant, loan, or cooperative agreement.
14. **Compliance with Prison Rape Elimination Act (PREA):** The contractor agrees to comply with all applicable provisions of the Prison Rape Elimination Act of 2003 (42 U.S.C. §§ 15601, et seq.), as amended from time to time, and National PREA Standards promulgated by the Attorney General of the United States, under authority of that Act, found at 28 CFR Part 115, as amended from time to time. The contractor further agrees to comply with all applicable administrative policies and procedures of the Kansas Department of Corrections and its facilities, dealing with the subject matter of sexual abuse or sexual harassment of inmates or juvenile residents.